أمن الاتصالات

بقلم القائد/ سيف العدل

هو مجموعة الإجـراءات الـتي تكفل منع العـدو من الحصول على معلومات عن طريق الاتصالات وتقـوم أيضا بمنعه من التدخل الفني أو التكتيكي على شبكة الاتصالات - التـدخل الفـني؛ عن طريق الـدخول في خط الهـاتف، التدخل التكتيكي؛ عن طريق فك الشفرة –

أولاً: الأخطار التي تواجه الاتصالات:

1) التصـنت عن طريق العملاء المجهـزين بـأجهزة خاصة للتجسس على الهاتف أو من خلال أمن السنترال.
2) القبض أو التفتيش.
3) الحوادث.

ثانياً: وسائل الاتصال المستخدمة:

1) السعاة:

السـعاة مفردها سـاعي وهو الشـخص الموكل إليه تحقيق الاتصــال بين الطــرفين باليد بينما يتم التأكد من نقل المعلومة أو الوثيقة عن طريق السلكي أو الإيصال.

أ) مزايا السعاة:

1) مؤمنة جداً.
2) التأكد من وصول المعلومة.
3) غير قابلة للكشف إلا في ظروف ضيقة جداً.

ب) عيوب السعاة:

1) تفتقد إلى السرعة.
2) الساعي عرضة للتجنيد من المعادين.
3) عرضة للحوادث أثناء النقل.

ج) تأمين السعاة:

1) اختيار الساعي على قدر من الخلق والاستقامة.
2) تحديد وتأمين المحاور التي يسلكها الساعي.

3) تـدريب العـاملين على كيفية إعـدام الوثـائق عند الخطر.
4) عدم الالتزام بتوقيت زمـاني أو مكـاني معين في نقل الرسائل.
5) تغيير السعاة باستمرار من آن لآخر.

2) البريد العادي:

وسـيلة نقل ممتـازة لكنها عرضة للسـرقة والرقابة وغـير سـريعة ويمنع اسـتخدامها في نقل الوثـائق والمعلومات الهامة جداً.

3) الحقيبة الدبلوماسية:

وسيلة مؤمنة بسبب الحصانة الدبلوماسية.

4) الاتصال السلكي - هاتف/ فـاكس/ تلكس - والهواتف النقالة:

اتصـالات سـريعة جـداً وكفاءتها عالية واسـتخداماتها واسـعة ولكنهـا عرضة للرصد والتصـنت ومكلفـة جـداً في تأمينها.

كيف يتم الرد على التليفون؟

من السـهل جـداً على جهـاز الاستخبارات الحصـول على معلومات بطريقة بسيطة منك كالآتي:

الاتصـال بـرقم هاتفك ومحاولة الحصـول على معلومات كالآتي:

أ) السؤال المغلوط: يقول لك: هل هذا أبو حسـين؟ يكون الرد: لا يا أخي، أبو حسين ليس موجود. فيقول لك: متى يأتي؟ هل هو مسافر؟

وهكذا قد يستطيع الحصـول منك على معلومات من خلال طريقة الحديث أو غيرها.

ب) يقـول لك: من معي؟ فيجيبه الأخ: معك أبو أحمـد، فيحـاول أن يسـألك بعض الأسـئلة الـتي يجمع من وراءها معلومات.

انتبه...

- لا تعط أي معلومات من خلال التليفون.
- لا تـذكر اسـمك أو معلومـات عن أي أخ آخـر، أو تعطي معلومات عن تحركات، أو وجود شخصٍ ما أو عـدم وجوده ، لا تعط أي بيانات.

الهواتف الثابتة والنقالة خطيرة جداً:

تعتبر الهواتف سواءً الثابت منها أو النقال من اخطر الأمور، وأكثر المعلومات التي يتحصل عليها العدو هي من الهـاتف، ومن أكـثر المـداخل الـتي يـؤتى المجاهـدون من قبلها هي الهواتـف، فكم من أخ تسـاهل في أمر الاتصـال وكم من أخ تســاهل في أمر كتابة الأرقــام ووضــعها في نوتة خاصة فإذا سـقطت سـقط معها الكثـير من الشـباب وأيضاً، لعل المتابع لحال الإخـوة في فلسـطين يـرى كيف استغل اليهود الهواتف النقالة في تصـفية واغتيـال الكثـير من القيـادات والكـوادر، فعلى الشـباب المجاهد تفـويت الفرصة على الأعداء وعـدم إكسـابهم أي أمر والله وحـده الحافظ من قبل ومن بعد.

بعض الأمثلة عن أخطاء حـدثت في عمليـات ضد الحكومـــات بســـبب التســـاهل في تـــامين الاتصالات:

المثال الأول: في عملية اغتيال حدثت في مصر - اشتبهت الحكومة المصرية في أن مدبري الحادث ينتمون إلى جماعة إسلامية في بيشاور - ولم تتمكن الحكومة من ضـــبط أحد في الحـــادث. فقـــامت الحكومة بوضع رقابة مشـددة على تليفونـات اعتـادت الجماعة الاتصـال بها في مصـــر، وبعد 3 أيـــام التقطت مكالمة من بيشــاور وهــذه المكالمة تحدد موعد للقـاء في القـاهرة وقـامت الحكومة بعمل كمين واعتقلت المسئولين عن الحادث.

المثـال الثـاني: عملية اغتيــال "شـهبور بختيـار" رئيس وزراء إيران السابق في فرنسا في عام 1992م :

كـــان "شـــهبور بختيـــار" يعيش في فيلا في فرنسا وعليه حراسة مشــددة من البــوليس الفرنسي لمــدة 24 ســـاعة متواصـــلة. زاره أحد العـــاملين المقـــربين منه والمعروف لطاقم الحراسة، وعندما وصل إلى فلته وكـان

معه اثنين آخرين إيرانيين سمح لهم البوليس بالدخول بعد تفتيشهم وتركوا جوازات سفرهم بالباب. دخلوا فحياهم "شهبور" وجلسوا ودخل سكرتير "شهبور" لإعداد الشاي في المطبخ فقفز هؤلاء على "شهبور" وقتلوه ثم قاموا بقتل السكرتير ومكثوا ساعة واحدة في الشقة ثم غادروا الفيلا وأخذوا جوازات سفرهم ورحلوا في السيارة.

ذهب معاون "شهبور" في طريق، والاثنان الآخران استقلوا القطار وتوجهوا إلى الحدود الفرنسية السويسرية لعبورها ولكن جمرك الحدود السويسري شك في تأشيرة الدخول إلى سويسرا ورفض السماح لهم بالدخول.

تحركوا إلى نقطة حدود أخرى ونجح أحدهما في الدخول إلى سويسرا ولم ينجح الآخر وبقي في داخل فرنسا هائماً على وجهه لمدة 5 أيام.

اكتشفت جثة "شهبور" بعد 48 ساعة من مقتله وقام البوليس بنشر صور المتهمين الثلاثة، وتم اعتقال الشخص الذي لم ينجح في الخروج من فرنسا، ولكنه أنكر صلته بالقتل وقال بأنه كان متواجداً فقط.

اشتبهت السلطات الفرنسية في أن الحكومة الإيرانية لها يد في هذه الجريمة فأرادت أن تثبت ذلك وقامت بعمل الآتي:

أ) قامت الحكومة بفحص جميع الكبائن العامة الموجودة على خط السير الذي تحرك فيه الرجلان في اتجاه الحدود السويسرية فأحصت أكثر من 20 ألف مكالمة في فترة الخمسة أيام قبل أن يتم القبض على هذا الرجل الذي لم يستطع الخروج.

ب) بعد الفحص الدقيق وجدت الحكومة تطابق في عدة مكالمات إلى شقتين في استنبول بتركيا وبالتالي تحددت هاتين الشقتين على أنهما مركز قيادة العملية.

ج) بعد ذلك طلبت الحكومة الفرنسية من الحكومة التركية المساعدة فقامت الحكومة التركية بفحص التليفونات الصادرة من هاتين الشقتين وهما مملوكتين لمواطن إيراني وأعطت البيانات إلى الاستخبارات الفرنسية وكانت المكالمات صادرة إلى:

- وزارة الخارجية الإيرانية.
- مكتب استخبارات إيـراني مسـئول عن العمليـات الخاصة.
- شـــقة في فرنسا؛ قـــامت السـلطات الفرنســية باســتجواب صــاحبتها فــاعترفت بأنهــا تعمل عميلــة مع الاستخبارات الإيرانية، تم فحص المكالمـات الصـادرة من شقة فرنسا وكانت صادرة إلى تركيا وإيران.

الخلاصة انه بمعرفة أرقام التليفونـات تم الربط بين المنفذين والحكومة الإيرانية

كيف تسيطر الحكومة على التليفون؟

التليفونــات تعمل بنظــام الكمــبيوتر، أي أن هنــاك كمــبيوتر مركــزي يســتطيع الــدخول على أي تليفــون أو إعطــاء بيانــات عن أي تليفــون في الدولة مثــل: أرقــام التليفونــات الــتي قــام هــذا التليفــون بالاتصــال بها لأنها مســجلة في الكمــبيوتر واسم صــاحب التليفــون وبياناته وهكذا...

وهذا تراه عندما تستلم فاتورة التليفون تكون كالآتي: هذه البيانات يصدرها الكمبيوتر:

مسلسل	رقم الهاتف		المكان	الوقت	عدد الدقائق	السعر
	من	إلى				
1	7009894	7065432	جدة	8:06	12	50 ريال

وهذا معناه أن جهـات الأمن تسـتطيع الحصـول على كل مكالمات تليفونك في أي وقت من السنة.

وبالنسبة للهاتف النقال:

فــإن جهــات الأمن تســتطيع بالإضــافة إلى معرفة مكالماتك تحديد مكانك عن طريق الذبذبات الـتي يرسـلها هاتفك النقال من وإلى البرج.

كيف تقـــــوم الدولة بالتصـــــنت العشـــــوائي على المكالمات التليفونية للشعب؟

المكالمـات التليفونية بـالملايين في وقت واحد وهي في الهـواء تماما مثل محطـات الإذاعة فـأنت عنـدما تفتح المذياع تسمع محطات و محطات و محطات..

نفس الشــيء الدولة لـديها أجهــزة تصــنت تســمى "متعدد القنوات " وهو عبارة عن جهاز كبير يقــوم العامل فيه بـــإدارة قـــرص مثل قـــرص الراديو ويضع في أذنيه سماعات فيستمع إلى المكالمات التليفونية المختلفة التي تقدر بالآلاف مثل الراديو والعامل يتوقف ويتابع المكالمـة، فإذا وجدها مكالمة عادية انتقل إلى مكالمة أخرى وهكذا.

إجراءات حماية الهواتف:

1) يفضل اسـتخدام هواتف الشـارع وعـدم التحـدث من الـبيت أو من الهـاتف النقـال أو من الفنـدق في حـال السفر.

2) لا تـــورط هاتفك ســـواءً الثـــابت أو النقـــال في الاتصالات لأن الاستخبارات ستعرف على من اتصـلت من خلال الفاتورة.

3) استغلال الفرص لتجنب الهواتف والتعــويض عنها بالاتصال المباشر إذا أمكن.

4) يمنع منعاً باتاً نقل أي معلومة سرية على الهاتف إلا مشفرة واستخدام الأسماء الحركية.

5) جعل المكالمة قصــيرة لا تتعــدى دقيقة واحـــدة ومن الأفضل كتابة المراد التحدث به قبل الاتصال.

6) عدم إعطاء أي بيانات لأي فرد يتحدث معك على الهاتف.

7) التفتيش عن أجهزة التصنت بصورة دورية.

8) تفقد حال الإخوة الذين يتم الاتصال عليهم عــادة حـــتى لا يتم القبض على أحـــدهم وتســـتمر المخـــابرات باستقبال المكالمات في بيته أو عبر هاتفه النقال.

9) حفظ الأرقـام ذهنيا أو تكتب بشـفرة لا يفهم أنها أرقام تليفونات.

10) الـــرد على التليفـــون بصـــيغة متفق عليها بين أفراد المكان الموجود فيه لمنع حـدوث أخطـاء ترشد عن أسماء وطبيعة ساكني هذا المكان.

11) عـــــدم جعل المكالمة مبهمةً وغامضةً، لأنه في هذه الحالة سوف يعتقد العامل أن هناك شـفرة سـرية أو أن هناك عملاً سرياً.

13) عـدم ذكر من أين يتحـدث الشـخص، لا يـذكر أسماء دول أو أماكن أحياء.

14) إذا كـــانت بلغة أجنبية وفي وقت قصـــير فإنها تكون أفضل لأن العامل قد يتجنبها.

15) عـــدم اسـتخدام التليفـــون من قبل شـــخص معـروف لـدى الدولة أو سـبق وأن رصد صـوته لأنه يوجد الان لدى الحكومات نظام مراقبة بصمة الصوت.

5) الاتصـــال اللاســـلكي - المخـــابرة أو ما يسمى بالآيكوم والكنود -

كفاءته ضـــعيفة ولا يعتمد عليه بالنســـبة لغـــيره من الاتصالات.

- مزايا اللاسلكي:

1) شبكة اتصال خاصة لا تتوفر لأي نوع آخر.
2) يمكن الإبـــداع فيها لتـــؤدي مهمتها بأمـــان لمن يستخدمها.
3) يوفر عامل السرعة.

- عيوب اللاسلكي:

1) أسهل ما يمكن في الالتقاط والتحديد.
2) أسهل ما يمكن التشويش عليه.

- تأمين الاتصال اللاسلكي:

1) اختيار الجهاز المناسب ويكون حر التردد.
2) الجهـــاز المناسب للغـــرض المناسب - الجهـــاز حسب المدى المطلوب ولا يزيد كثيراً عنه -
3) تغيير الترددات والكود باستمرار.

4) اختيــار الأفــراد القــائمين على الأجهــزة بعناية ومراقبتهم.
5) اختيار شفرة مناسبة - للمكالمة أو الجهاز -

6) لمنع الالتقاط والتحديد يتبع الآتي:

أ) عدم الاتصال إلا عند الضرورة.
ب) عدم تحديد موعد الاتصال كموعد ثابت.
ج) تقليل مدة الاتصال قدر الإمكان.
د) استخدام أقل طاقة ممكنة للجهاز وتؤدي الغرض المطلوب.
هـ) استخدام هوائي موجه.

7) لمنع التشويش يتم اتباع الآتي:

أ) يتم الاتصـــال على ذبذبة ثابتة مع وجــــود ذبذبة احتياطية متفق عليها بكــــود وليس صــــراحة بحيث يتم الانتقال إليها عند التشويش.
ب) تغيير مكان الاتصال كلما أمكن ذلك.
ج) عدم الاتصال يوميا.

8) اختيار عدة موجات ومراقبتها جيدا للتأكد من عدم استخدامها من قبل أحد.

<u>ملاحظات:</u>

1) الإهمال في الاتصال باهظ الثمن تماماً.
2) الأتصــال اللاســلكي - المخــابرة - خطر جــداً ولا يستخدم إلا في الضرورة وبتشفير دقيق.

عن معسكر البتار
العدد الخامس / محرم 1425 هـ